

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-006880

(43)Date of publication of application : 10.01.1997

(51)Int.Cl.

G06F 19/00
G06F 15/00
G07F 7/12
// G07B 1/00

(21)Application number : 08-203359

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

(22)Date of filing : 01.08.1996

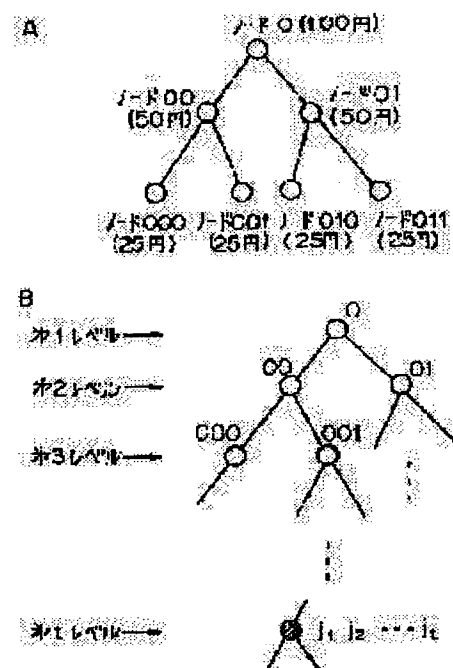
(72)Inventor : OKAMOTO TATSUAKI
OTA KAZUO

(54) METHOD FOR DIVISIONAL USE OF ELECTRONIC CASH

(57)Abstract:

PROBLEM TO BE SOLVED: To enable the divisional use of electronic cash.

SOLUTION: A hierarchical structure table which has the face value (e.g. 100 yen) of the electronic cash set at the top and a use minimum unit (e.g. 75 yen) at the bottom is generated, and a rule wherein (1) the total of the corresponding amounts of child nodes right below one node is equal to the amount of the node and (2) when one node is used once, all the ancestor nodes and descendant nodes connected to the node are not used is applied. For example, when 75 yen is used, nodes 00 and 010 are used.



LEGAL STATUS

[Date of request for examination]

01.08.1996

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the
examiner's decision of rejection or application
converted registration]

[Date of final disposal for application]

[Patent number]

2879792

[Date of registration]

29.01.1999

[Number of appeal against examiner's decision of
rejection][Date of requesting appeal against examiner's decision
of rejection]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-6880

(43) 公開日 平成9年(1997)1月10日

(51) Int.Cl. ^a	識別記号	序内整理番号	F I	技術表示箇所
G 0 6 F 19/00			G 0 6 F 15/30	3 4 0
15/00	3 9 0	9364-5L	15/00	3 9 0
G 0 7 F 7/12			G 0 7 B 1/00	E
// G 0 7 B 1/00			G 0 6 F 15/30	Z
				3 6 0

審査請求 有 請求項の数 3 O L (全 12 頁) 最終頁に続く

(21) 出願番号 特願平8-203359
(62) 分割の表示 特願平3-143530の分割
(22) 出願日 平成3年(1991)6月14日

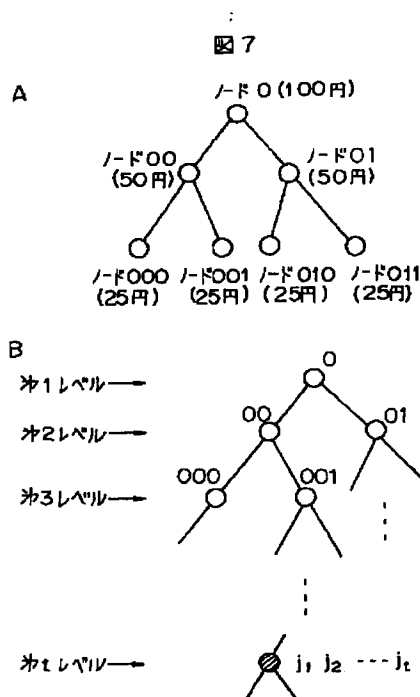
(71) 出願人 000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番2号
(72) 発明者 岡本 龍明
東京都千代田区内幸町一丁目1番6号 日
本電信電話株式会社内
(72) 発明者 太田 和夫
東京都千代田区内幸町一丁目1番6号 日
本電信電話株式会社内
(74) 代理人 弁理士 草野 卓

(54) 【発明の名称】 電子現金の分割使用方法

(57) 【要約】

【課題】 電子現金の分割使用を可能とする。

【解決手段】 電子現金の額面（例えば100円）を階層的構造テーブルの最上位とし、使用最小単位（例えば75円）を階層的構造テーブルの最下位層としたテーブルを定め、（1）このテーブルにはあるノードの直下の子ノードの該当金額の合計が、そのノードの該当金額となる、（2）あるノードが一度使われた後は、そのノードと連結するすべての先祖ノードにおよび子孫ノードは利用しないというルールを適用する。例えば75円を使う場合は、ノード00とノード010を用いる。



1

【特許請求の範囲】

【請求項1】 電子現金の額面を階層的構造テーブルの最上位ノードとし、使用最小単位を階層的構造テーブルの最下位層のノードとし、あるノードの直下の子ノードの該当金額の合計が、そのノードの該当金額とする階層的構造テーブルを定め、

使用金額をノードで指定し、

あるノードが一度使われた後は、そのノードのすべての先祖ノード、およびすべての子孫ノードは利用しない、かつ各ノードは1回以上使用しないというルールを適用する電子現金の分割使用方法。

【請求項2】 電子現金を利用する者（以下、利用者という）が有する装置（以下、利用者側装置という）と、利用者より電子現金を受領する機関（以下、小売店という）が有する装置（以下、小売店側装置という）により電子現金を分割使用する請求項1記載の方法において、上記利用者側装置は電子現金の額面と対応した値 Γ を生成し、上記階層構造における使用金額と対応したノードと対応した値 $\Omega_{j_1 \dots j_t}$ を生成し、

上記値 Γ と上記値 $\Omega_{j_1 \dots j_t}$ ($L=1, \dots, t$)を用いて、上記使用金額に対応するノードに対する値の剰余べき乗根

【数1】

$$X_{j_1 \dots j_t} = \left[(\Omega_{j_1 \dots j_{t-1}}^{2^{t-1}j_t} \Omega_{j_1 \dots j_{t-2}}^{2^{t-2}j_{t-1}} \dots \Omega_{j_1}^{2j_2} \Gamma_0)^{1/2^t} \bmod N \right]_{-1}$$

を求め、 $[\dots]_{-1}$ はヤコビ記号であって、 $(x_1 \dots x_t / N) = -1$ であり、

この $x_1 \dots x_t$ および電子現金を上記小売店側装置へ送り、

上記小売店側装置は上記受信した $x_1 \dots x_t$ が $(x_{j_1 \dots j_t} / N) = -1$ を満たすかを検証し、

利用者側装置と同様の処理により Γ と $\Omega_{j_1 \dots j_t}$ を生成し、

【数2】

$$X_{j_1 \dots j_t}^{2^t} = d \Omega_{j_1 \dots j_{t-1}}^{2^{t-1}j_t} \Omega_{j_1 \dots j_{t-2}}^{2^{t-2}j_{t-1}} \dots \Omega_{j_1}^{2j_2} \Gamma_0 \bmod N$$

を満たすかを検証し、

以上の検証が正しければ、上記電子現金による上記使用金額の支払いを認める。

【請求項3】 電子現金を利用する者（以下、利用者という）が有する装置（以下、利用者側装置という）と、

利用者より電子現金を受信する機関（以下、小売店という）が有する装置（以下、小売店側装置という）により電子現金を分割使用する請求項1または2記載の方法において、

小売店側装置は値 E ($=0$ または 1)を利用者側装置へ送り、

2

利用者側装置は電子現金の額面および使用金額ノードと対応した値 $\Lambda_{j_1 \dots j_t}$ を生成し、

値 $\Lambda_{j_1 \dots j_t}$ と値 E とから次の剰余平方根演算を行い、 $Y_{j_1 \dots j_t} = \{ (\Lambda_{j_1 \dots j_t})^{E/2} \bmod N \}_{(-1)^E}$

この $Y_{j_1 \dots j_t}$ を小売店側装置へ送り、

小売店側装置は受信した $Y_{j_1 \dots j_t}$ について

$$(Y_{j_1 \dots j_t} / N) = (-1)^E$$

$$(Y_{j_1 \dots j_t})^2 = d' f \Lambda (C_{j_1} \parallel \dots \parallel C_{j_t} \parallel N) \bmod N$$

を共に満足するかを検証し、正しければ上記電子現金による上記使用金額の支払いを認める。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、電気通信システムやICカードなどを用いて電子現金による支払い、譲渡などを行う際に、電子現金をその額面の範囲内で分割使用する電子現金の分割使用方法に関する。

【0002】

【従来の技術】電気通信システムを用いた電子資金移動が普及しつつある。一般に換金可能な証書（手形、小切手など）は、証書の象徴的機能（証書を保持している人に対して、証書に記載してある権利が供与されること）を備えている。証書を電気通信システムで取り扱う場合、証書はデジタル化されたデータであり、容易にコピーを作成して複数回の換金が可能となる。プリペイドカードのような電子的現金を実現するときにも、この問題が生じる。すなわち、プリペイドカードをコピーすることで、不正に複数回の換金あるいは商品の購入が可能となる。一方、クレジットカードでは、このような2重使用の危険性はほとんどないが、その代わりに、利用者の利用履歴がすべてカード会社に知られてしまうという欠点がある（つまり、プライバシーが保証されていない）。

これら問題の解決策として、計算機能を備えたカードで換金時にカード読み取り装置とカードとの間のデータのやりとりを工夫することで、プライバシーを保証し、かつカードの2重使用を検出する方法が提案されている。たとえば、Chaum, Fiat, Naor:

"Untraceable Electric Cash", Proc. of CRYPTO'88がある。しかしながら、Chaum等の方式では、一回発行された電子現金を分割して利用する（例えば、1万円の電子現金を合計利用額が1万円になるまで何回も利用する）ことはできない。また、Chaum等の方式では、一回毎の電子現金発行時に、銀行と利用者の間でかなりの量の通信と処理を行う必要がある。

【0003】

【発明が解決しようとする課題】この発明の目的は、一回発行された電子現金を発行時に決められた額になるまで、何回も分割して利用できる電子現金の分割利用方法を提供することにある。

【0004】

【課題を解決するための手段】請求項1の発明によれば、電子現金の額面を階層的構造テーブルの最上位ノードとし、使用最小単位を階層的構造テーブルの最下位層のノードとし、あるノードの直下の子ノードの該当金額の合計が、そのノードの該当金額とする階層的構造テーブルを定め、使用金額をノードで指定し、あるノードが一度使われた後は、そのノードのすべての先祖ノード、およびすべての子孫ノードは利用しない、かつノードは1回以上使用しないというルールを適用することにより電子現金の分割使用を可能とする。

【0005】請求項2の発明によれば、電子現金を利用する者（以下、利用者という）が有する装置（以下、利用者側装置という）と、利用者より電子現金を受信する機関（以下、小売店という）が有する装置（以下、小売店側装置という）により電子現金を分割使用する請求項1記載の方法において、上記利用者側装置は電子現金の額面と対応した値 Γ を生成し、上記階層構造における使用金額と対応したノードと対応した値 Ω_{j_1, \dots, j_t} を生成し、上記値 Γ と上記値 Ω_{j_1, \dots, j_t} （ $L=1, \dots, t$ ）を用いて、上記使用金額に対応するノードに対する値の剰余べき乗根

【0006】

【数3】

$$X_{j_1 \dots j_t} = \left[(\Omega_{j_1 \dots j_{t-1}}^{2^{t-1} j_t} \Omega_{j_1 \dots j_{t-2}}^{2^{t-2} j_{t-1}} \dots \Omega_{j_1}^{2 j_2} \Gamma_0)^{1/2^t} \bmod N \right]_{-1}$$

【0007】を求め、 $[\dots]_{-1}$ はヤコビ記号であって、 $(x_1 \dots x_t / N) = -1$ であり、この $x_1 \dots x_t$ および電子現金を上記小売店側装置へ送り、上記小売店側装置は上記受信した $x_1 \dots x_t$ が $(x_1 \dots x_t / N) = -1$ を満たすかを検証し、利用者側装置と同様の処理により Γ と Ω_{j_1, \dots, j_t} を生成し、

【0008】

【数4】

$$X_{j_1 \dots j_t}^{2^t} = d \Omega_{j_1 \dots j_{t-1}}^{2^{t-1} j_t} \Omega_{j_1 \dots j_{t-2}}^{2^{t-2} j_{t-1}} \dots \Omega_{j_1}^{2 j_2} \Gamma_0 \bmod N$$

【0009】を満たすかを検証し、以上の検証が正しければ、上記電子現金による上記使用金額の支払いを認める。つまりあるノードが一度使われた後は、そのノードと連結するすべての先祖ノードおよび子孫ノードは利用しないことを満たしていると認める。

【0010】請求項3の発明によれば、電子現金を利用する者（以下、利用者という）が有する装置（以下、利用者側装置という）と、利用者より電子現金を受信する機関（以下、小売店という）が有する装置（以下、小売店側装置という）により電子現金を分割使用する請求項1または2記載の方法において、小売店側装置は値E（=0または1）を利用者側装置へ送り、利用者側装置

は電子現金の額面および使用金額ノードと対応した値 $\Lambda_{j_1, \dots, j_t}$ を生成し、値 $\Lambda_{j_1, \dots, j_t}$ と値Eとから次の剰余平方根演算を行い、

$$Y_{j_1, \dots, j_t} = \left[(\Lambda_{j_1, \dots, j_t})^{E/2} \bmod N \right]_{(-1)^E}$$

この Y_{j_1, \dots, j_t} を小売店側装置へ送り、小売店側装置は受信した Y_{j_1, \dots, j_t} について

$$(Y_{j_1, \dots, j_t} / N) = (-1)^E$$

$$(Y_{j_1, \dots, j_t})^2 = d' f \Lambda (C \| j_1 \| \dots \| j_t \| N) \bmod N$$

10 を共に満足するかを検証し、正しければ上記電子現金による上記使用金額の支払いを認める。つまりノードの直下の子ノードの該当金額の合計が、そのノードの該当金額となるという条件を満たしていることになる。

【0011】つまり、この発明においては、電子現金の構造に対応した階層構成のテーブルを構成し、電子現金利用時には、このテーブルの構造に対応させる形で、一定の額面金額内の現金を何回かに分割して使用可能としている。また、上記利用形態における不正使用を検出するため、上述のように利用者と小売店との確認で剰余べき乗根を利用することは、例えばウィリアムズ数と呼ばれる合成数を法とする偶数べき乗根を利用することであり、ここでは、2つの異なるタイプの偶数べき乗根を用いて、法である合成数の素因数分解ができるという事実が重要な役割をする。つまり、利用者が不正使用をすれば、法の素因数分解を通じて、利用者の秘密情報である利用者のIDが露見するしかけになっている。

【0012】

【発明の実施の形態】

（1）まず電子現金の発行および使用するためのシステム構成の例を図1に示す。電子現金を発行する機関（以下、銀行という）の装置（以下、銀行側装置という）100と、電子現金を発行される者（以下、利用者という）の装置（以下、利用者側装置という）200と、利用者より電子現金を受領する機関（以下、小売店という）の装置（以下、小売店側装置という）300とが通信回線等を介して接続している。

【0013】（2）次に電子現金の利用者のプライバシーを保証するために用いる利用許可証の発行処理について説明する。まず、銀行で口座を新たに開設した利用者が、利用許可証を銀行より発行してもらう場合について説明する。利用者側装置は利用者の識別情報IDp（利用者の口座番号など）を含んだ秘密情報（利用者情報）より乱数で攪乱したK組のブラインド情報を作成し、銀行側装置は、そのブラインド情報の中でK/2組の情報の開示を求め、開示された情報が正しく作成されていれば、残りの未開示のK/2組の情報に対しブラインド署名を作成し利用者側装置に送信し、利用者側装置は、銀行側装置から受信したブラインド署名から利用者情報に対する銀行の署名を計算して、この銀行署名を利用許可証とする。

【0014】銀行側装置は、利用許可証に対応する情報として、デジタル署名で用いるRSA暗号の秘密鍵 (dA, nA) および公開鍵 (eA, nA) の対を作成しておき、公開鍵 eA, nA を公開しておく。一方、利用者側装置は、デジタル署名で用いるRSA暗号の秘密鍵 (dP, nP) および公開鍵 (eP, nP) の対を作成しておき、 (eP, nP) をIDPと対にして公開しておく。

【0015】利用者が銀行から利用認可証を発行してもらう手順は、以下の通り。銀行側装置と利用者側装置の間の通信例を図2に示す。利用者側装置200の利用許可証発行処理の構成を図3に、銀行側装置のそれを図4にそれぞれ示す。以下では、 $i = 1, 2, \dots, K$ とする。

ステップ1 利用者側装置は、乱数発生器201を用いて乱数 a_i, r_i を生成して、IDPと共に連結器204に入力し、その出力 $IDP \parallel a_i$ を一方方向ハッシュ関数演算器205に入力し、さらにその出力 $q(IDP \parallel a_i)$ を利用者の署名用秘密鍵 (dP, nP) と共にRSA署名器206に入力し、 $(q(IDP \parallel a_i))^{dP \bmod nP}$ を求める。

【0016】ステップ2 署名器206の出力をIDP、 $\parallel a_i$ と共に連結器207に入力して、 $S_i = IDP \parallel a_i \parallel (q(IDP \parallel a_i))^{dP \bmod nP}$ を求める。さらに、 S_i を分割器208に入力し、 $S_i = S_{1,i} \parallel S_{2,i}$ になるような $S_{1,i}$ と $S_{2,i}$ を求める。

ステップ3 素数生成器202を用いて、 $P_i \equiv 3 \pmod{8}$ および $Q_i \equiv 7 \pmod{8}$ を満足する2つの素数 P_i, Q_i を生成して、乗算器203を用いてその積 $N_i = P_i \cdot Q_i$ を求める。

【0017】ステップ4 $S_{1,i}$ および $S_{2,i}$ を N_i と共に剰余べき乗演算器209および211にそれぞれ入力し、 $I_{1,i} = (S_{1,i})^2 \bmod N_i$ と $I_{2,i} = (S_{2,i})^2 \bmod N_i$ を求め、それらを連結器210に入力し $I_i = I_{1,i} \parallel I_{2,i}$ を計算する。

ステップ5 N_i, I_i を連結器212に入力し、その出力 $I_i \parallel N_i$ を一方方向ハッシュ関数演算器213に入力し、 $q(I_i \parallel N_i)$ を得る。一方、 r_i を銀行の公開鍵 (eA, nA) と共にRSA暗号器215に入力し、 $(r_i)^{eA \bmod nA}$ を求める。次に、それら出力を剰余乗算器214に入力し、ブラインド情報 $W_i = (r_i)^{eA \bmod nA} \cdot q(I_i \parallel N_i) \bmod nA$ を求めて、 W_i ($i = 1, 2, \dots, K$)を銀行側装置に送信する。

【0018】ステップ6 次に、銀行側装置は、利用者側装置に、そのうちの $K/2$ 組の a_i, P_i, Q_i ($q(IDP \parallel a_i))^{dP \bmod nP}, IDP, r_i$ を開示させて、利用者側装置がステップ1からステップ5を正しく実行していることを確認する。このため、銀行側装置100は、1からKの中からランダムに $K/2$ 個を選び、それを開示要求として利用者側装置に送信する(ここでは、表記を簡単にするため、 $K/2 + 1, K/2 + 2,$

..., K が開示指定されたと仮定して説明する)。 $K/2$ 個でなく、 K の一部であればよいが、 $K/2$ とすると処理効率が良い。

【0019】ステップ7 利用者側装置200は、銀行側装置から開示要求を受信すると、銀行側装置の指示する $K/2$ 組の $a_i, P_i, Q_i, (q(IDP \parallel a_i))^{dP \bmod nP}, IDP, r_i$ を開示する。銀行側装置は、 i が開示対象の時、次の手順を行う。

ステップ8 利用者側装置200より受信した a_i, IDP より $(q(IDP \parallel a_i))^{dP \bmod nP}$ の署名の正当性を利用者側装置の公開鍵 (eP, nP) を用いて連結器104で a_i とIDPを連結し、それを一方方向ハッシュ関数演算器105へ供給し、一方 $(q(IDP \parallel a_i))^{dP \bmod nP}$ と nP, eP とをRSA暗号器107に入力して暗号化しこの結果と演算器105の出力とを比較器111で検証する。ここで、検証に合格しなければ処理を中断する。

【0020】ステップ9 利用者側装置200より受信した $a_i, P_i, Q_i, (q(IDP \parallel a_i))^{dP \bmod nP}, IDP$ から、乗算器103を用いて $N_i = P_i \cdot Q_i$ を求め、さらに、連結器108で a_i, IDP を連結して S_i とし、 S_i を分割器109で分割し、それぞれ剰余べき乗演算器110, 112で N_i と剰余べき乗演算し、その結果を連結器111で連結して I_i を求める。

【0021】ステップ10 上で計算した I_i, N_i を連結器113で連結し、更に一方方向ハッシュ関数演算器114に供給し、受信した r_i と公開鍵 eA, nA をRSA暗号器117へ供給し、その出力と演算器114の出力とを剰余乗算器115へ供給して $W'_i = (r_i)^{eA \bmod nA} \cdot q(I_i \parallel N_i) \bmod nA$ を計算する。

ステップ11 前に受信した W_i の値と W'_i の値を比較器116で比較し、一致すれば合格とし、不合格の場合、処理を中断する。銀行側装置は、 $K/2$ 個のすべての i について上記の検査を行い、いずれかの検査に不合格のときには、以降の処理を中止する。すべての検査に合格のときには、銀行側装置は、開示対象でない $i = 1, \dots, K/2$ に対して、次の手順でブラインド署名を行う。

【0022】ステップ12 剰余乗算器118とRSA署名作成器119を用いて、銀行側装置の署名用秘密鍵 (nA, dA) と W_i とから $W = (\prod W_i)^{dA \bmod nA}$ を求め、つまりブラインド署名を作り、この W を利用者側装置に送信する。

ステップ13 利用者側装置は、銀行側装置から W を受信すると、 r_i と公開鍵 (eA, nA) から、剰余乗算器216、剰余除算器217を用いて利用許可証 $B = W / (\prod r_i) \bmod nA = (\prod q(I_i \parallel N_i))^{dA \bmod nA}$ を計算する。 \prod は $i = 1$ から $K/2$ までである。

【0023】(3)更に利用許可証を用いて電子現金を発行してもらう処理を説明する。次に、利用者が銀行か

ら電子現金を発行してもらう手順を示す。まず、銀行側装置は、電子現金の金額に対応する情報として、RSAデジタル署名で用いる秘密鍵(d_A', n_A')および公開鍵(e_A', n_A')の対を作成しておき、(e_A', n_A')をその金額と共に公開しておく。ここで、銀行側装置と利用者側装置の間の通信例を図5に示す。利用者側装置200および銀行側装置100の各電子現金発行処理の構成を図6A、Bにそれぞれ示す。以下では、 $i = 1, 2, \dots, K/2$ とする。

【0024】ステップ1 乱数発生器201を用いて生成した乱数 b 、 r と利用許可証Bおよび電子現金の発行金額に相当する銀行側装置の公開鍵(e_A', n_A')から r と e_A', n_A' とをRSA暗号器215へ供給して認証用情報を生成し、これと h 、Bとから連結器204、一方方向ハッシュ関数演算器205、剰余乗算器214を用いて、

$$Z = r^{e_A'} \cdot g(B \parallel b) \bmod n_A'$$

を計算して引き出す電子現金の金額に相当するブラインド情報を得る。

【0025】ステップ2 この Z を電子現金の金額情報と共に銀行側装置へ送る。

ステップ3 Z を受信した銀行側装置は、 Z と電子現金の金額に対応する秘密鍵(d_A', n_A')とをRSA署名生成器119に入力し、 $Z' = Z^{d_A'} \bmod n_A'$ を求め、つまり引出し金額に相当するブラインド署名を作成してそれを利用者側装置に送付する。同時に、利用者側装置の口座から該当する金額を引き落とすか、利用者側装置から該当する金額を受領する。

【0026】ステップ4 銀行側装置より Z' を受信した利用者は、乱数 r と銀行側装置より受信した情報 Z' および公開鍵 n_A' 剰余除算器217に入力し、認証用情報および利用許可証に対する銀行側装置の署名 $C = Z' / r \bmod n_A' = (g(B \parallel b))^{d_A'} \bmod n_A'$ を求める。ここで、 C が電子現金に相当する。

【0027】(4)以上のようにして発行された電子現金をこの発明により分割使用する方法を説明する。利用者が、電子現金を用いて小売店で支払いをする場合について説明する。まず、電子現金の金額およびその使用最小単位(例えば、10円単位等)に対応して、階層的構造テーブルが定められる。たとえば、25円単位で、1

00円の紙幣を利用する場合の階層的構造テーブルを図7Aに示す。電子現金の額面100円は階層的構造テーブルの最上位とされ、使用最小単位25円は階層的構造テーブルの最下位層とされる。ここで、例えば、75円を使う場合、ノード00とノード010が該当するノードとなる。この該当ノードは、以下のルールで定められる。

【0028】1. あるノードの直下の子ノードの該当金額の合計が、そのノードの該当金額となる。

2. あるノードが一度使われた後は、そのノードと連結するすべての先祖ノードおよび子孫ノードは利用してはならない。

3. 各ノードは、一回以上使用してはならない。

【0029】このルールに従うと、先の例では、ノード00とノード010が使用された後で、使用できるノードは、ノード011(25円)のみである。つまり、上のルールに従うことにより、使用できる合計金額は、額面通り100円となると共に、25円単位でどのような使い方ででもできる。この階層的構造テーブルは、電子現金の額面金額を大きくし、さらに利用単位金額を小さくすれば、その階層が増えることになる。例えば、額面が100万円で、1円単位で利用できる電子現金の場合、その階層は、およそ20となる($\log_2 1000000 \div 20$)。

【0030】次に、利用者側装置と小売店側装置の間の通信例を図8に示す。小売店側装置300と利用者側装置200の電子現金利用手続の処理構成をそれぞれ図9、10に示す。多くの場合、利用金額に相当する階層構造テーブルの該当ノードは複数あるが、各ノードに対応する処理は、基本的に同じアルゴリズムで行われ、それぞれのノードの処理を並列に行うことができるため、以下では、1つのノードに対する処理のみを説明する。この該当ノードをノード j_1, j_2, \dots, j_t ($j_i \in \{0, 1\}$)とする(図7B)。また、以下では、 $i = 1, 2, \dots, K/2$ とする。

【0031】なお、以下の手順で用いる記号の意味をここでまとめて記しておく。

【0032】

【数5】

9

10

$$\left[x^{1/2^t \bmod N} \right]_1 = y'$$

では、 $y'^{2^t} = x \bmod N$, $(y'/N)=1$, かつ $0 < y' < N/2$. (1≦t)

$$\left[x^{1/2^t \bmod N} \right]_{-1} = y''$$

では、 $y''^{2^t} = x \bmod N$, $(y''/N)=-1$, かつ $0 < y'' < N/2$. (1≦t)

$$\langle z \rangle_{QR} = dz \bmod N$$

では、 $d \in \{\pm 1, \pm 2\}$ かつ dz が N に関し平方剰余。

$$\langle z \rangle_1 = d'z \bmod N$$

では、 $d' \in \{1, 2\}$ かつ $(d'z/N) = 1$.

$$\langle z \rangle_{-1} = d''z \bmod N$$

では、 $d'' \in \{1, 2\}$ かつ $(d''z/N) = -1$.

【0033】なお、以上において、(／)は、ヤコビ記号を意味する。ヤコビ記号の効率的計算法は、例えば、藤崎、森田、山本著の「数論への出発(数学セミナー増刊)」(日本評論社)の166頁に記されている。

ステップ1 利用者側装置200は、まず、 C , N_i よりランダム関数 Γ 演算器220を用いて、 $\Gamma_{i,0}$ を求める。

【0034】

【数6】

$$\Gamma_{i,0} = \langle f_r(C \| 0 \| N_i) \rangle_{QR}$$

【0035】次に、 C と利用金額と対応するノード j_1, \dots, j_t と N_i をランダム関数 Ω 演算器221に入力し、 $\Omega_{i,j_1 \dots j_t}$ ($L=1, \dots, t$)を生成する。

【0036】

【数7】

$$\Omega_{i,j_1 \dots j_t} = \langle f_a(C \| j_1 \| \dots \| j_t \| N_i) \rangle_1$$

【0037】さらに、 $\Gamma_{i,0}$, $\Omega_{i,j_1 \dots j_t}$ ($L=1, \dots, t$), N_i より剰余べき乗演算器222、剰余乗算器223、剰余べき乗根演算器224を用いて、利用金額に対応するノードに対する値の剰余べき乗根 $X_{i,j_1 \dots j_t}$ を求める。ここで N_i はウィリアムズ数である。

【0038】

【数8】

$$X_{i,j_1 \dots j_t} = \left[\left(\Omega_{i,j_1 \dots j_{t-1}}^{2^{t-1}j_t} \Omega_{i,j_1 \dots j_{t-2}}^{2^{t-2}j_{t-1}} \dots \Omega_{i,j_1}^{2j_2} \Gamma_{i,0} \right)^{1/2^t} \bmod N_i \right]_{-1}$$

【0039】ステップ2 利用者側装置200は、 b , $(I_i, N_i, X_{i,j_1 \dots j_t})$ ($i=1, \dots, K/2$)および (B, C) を小売店側装置300に送る。

ステップ3 小売店側装置300は、連結器304、一方向ハッシュ関数演算器305、剰余乗算器309、R

SA暗号器310、比較器311を用いて、公開鍵 (e, nA) により B の $I_i \| N_i$ に対する署名の正当性を(つまり、 $B^{*A} = (\prod g(I_i \| N_i)) \bmod nA$ が成立するかどうかを、 \prod は $i=1$ から $K/2$ まで)、また、連結器312、一方向ハッシュ関数演算器313、RSA暗号器314、比較器315を用いて公開鍵 (eA', nA') により C の $B \| b$ に対する署名の正当性を(つまり、 $C^{*A'} = (g(B \| b)) \bmod nA'$ が成立するかどうかを)検査する。この検査が、不合格のときは以降の処理を中止する。

【0040】ステップ4 小売店側装置300は、ヤコビ記号演算器316および比較器317を用いて、 $X_{i,j_1 \dots j_t}$ が以下の関係を満足するかどうかを検証する。この検査が、不合格のときは以降の処理を中止する。

$$(X_{i,j_1 \dots j_t} / N_i) = -1,$$

次に、 C , N_i よりランダム関数 Γ 演算器324を用いて、

【0041】

【数9】

$$f_r(C \| 0 \| N_i)$$

【0042】を求める。また、 C , j_1, \dots, j_t , N_i をランダム関数 Ω 演算器321に入力し、 $\Omega_{i,j_1 \dots j_t}$ ($L=1, \dots, t$)を生成する。

【0043】

【数10】

$$\Omega_{i,j_1 \dots j_t} = \langle f_a(C \| j_1 \| \dots \| j_t \| N_i) \rangle_1$$

【0044】さらに、

【0045】

【数11】

$$f_r(C \| 0 \| N_i), \Omega_{i,j_1 \dots j_t} \quad (l=1, \dots, t), N_i$$

【0046】より剰余べき乗演算器322、剰余乗算器

323、剰余除算器319、比較器320を用いて、 $X_{i,1,1, \dots, 1,t}$ が以下の関係を満足するかどうかを検証する。この検査が、不合格のときは以降の処理を中止する。つまり、あるノードが一度使われた後は、そのノードと連結するすべての先祖ノードおよび子孫ノードは利用してはならないというルール2を満たしているかが検証される。

【0047】

【数12】

$$X_{i,j_1 \dots j_t}^{2^t} = d_i \Omega_{i,j_1 \dots j_{t-1}}^{2^{t-1}} \Omega_{i,j_1 \dots j_{t-2}}^{2^{t-2}} \dots \Omega_{i,j_1}^{2j_2} \Gamma_{i,0} \bmod N_i$$

【0048】ここで、 d_i は、 ± 1 、 ± 2 のいずれかの値である。

ステップ5 小売店側装置は、乱数発生器301より取り出した値 $E_i \in \{0, 1\}$ ($i = 1, \dots, K/2$)を利用者側装置に質問情報として送付する。

ステップ6 利用者側装置は、ランダム関数 Λ 演算器225を用いて、 C, j_1, \dots, j_t, N_i より $\Lambda_{i,1,1, \dots, 1,t}$ を計算する。

【0049】

【数13】

$$\Lambda_{i,j_1 \dots j_t} = \langle f_{\Lambda}(C \| j_1 \| \dots \| j_t \| N_i) \rangle_{QR}$$

【0050】次に、剰余平方根演算器226を用いて、 $\Lambda_{i,1,1, \dots, 1,t}$ および E_i より、 $Y_{i,1,1, \dots, 1,t}$ を計算する。

【0051】

【数14】

$$Y_{i,j_1 \dots j_t} = \left[(\Lambda_{i,j_1 \dots j_t})^{1/2} \bmod N_i \right]_{(-1)^{E_i}}$$

【0052】利用者側装置は、 $Y_{i,1,1, \dots, 1,t}$ を小売店側装置に送る。

ステップ7 小売店は、ヤコビ記号演算器325および比較器326を用いて、 $Y_{i,1,1, \dots, 1,t}$ が以下の関係を満足するかどうかを検証する。この検査が、不合格のときは以降の処理を中止する。

$$(Y_{i,1,1, \dots, 1,t} / N_i) = (-1)^{E_i}$$

次に、 C, j_1, \dots, j_t, N_i をランダム関数 Λ 演算器328に入力し、さらにその出力および $Y_{i,1,1, \dots, 1,t}, N_i$ に対し、剰余べき乗演算器327、剰余除算器329、比較器330を用いて、以下の関係を満足するかどうかを検証する。

【0053】

【数15】

$$(Y_{i,j_1 \dots j_t})^2 = d'_i f_{\Lambda}(C \| j_1 \| \dots \| j_t \| N_i) \bmod N_i$$

【0054】ここで、 d'_i は、 ± 1 、 ± 2 のいずれかの値である。この検査に合格すれば、小売店側装置は、

その電子現金のノード j_1, \dots, j_t に該当する金額の支払を正当なものとし、それを受け取る。つまり、これらの検証によりあるノードの直下の子ノードの該当金額の合計が、そのノードの該当金額となるというルール1の条件を満たしているかの検証を行っている。

【0055】(5) 決済

最後に、小売店と銀行の間の決済方法について説明する。小売店側装置300は、利用者側装置200との電子現金利用時の交信履歴 H を銀行側装置に提出し、銀行側装置から該当する金額の支払いを受ける。銀行側装置は、 H の正当性を検査し、検査に合格すれば、 H を記憶して、小売店の口座へ該当する金額を払い込む。銀行側装置は、電子現金の不正利用を見つけると、 H を取り出して、それらの情報より不正者のIDを確定する。

【0056】つまり第21段落に記載されたルール2、に違反した場合、子ノードに対応する X を2乗してゆき、親ノードの平方根でヤコビ記号が1となるものを得ることと、親ノードに対応する X は、親ノードの平方根でヤコビ記号が-1となるものであることから、ヤコビ記号が1となる平方根と-1となる平方根が揃ったことにより、 N を素因数分解することができ、 N の素因数を用いて、 I から利用者の秘密情報 S を計算でき、またルール3、に違反した場合、 E はランダムに1か-1かが指定されたものであり、 Y は Λ の平方根でヤコビ記号が E により指定されたものだから、同じ Λ を用いて Y を生成すると、 $1/2$ の確率でヤコビ記号が1と-1となる平方根が揃うことになり、 $K/2$ 個の添字 i について手続きを実行すれば、ヤコビ記号が1となる平方根と-1となる平方根が圧倒的確率で揃うことにより、 N を素因数分解することができ、 N の素因数を用いて、 I から利用者の秘密情報 S を計算できる。

【0057】上述において、利用許可証 B 、電子現金 C に対する検証は他の手法を用いてもよく、従って上述において $i = 0$ としてもよい。

【0058】

【発明の効果】この発明は、階層的構造テーブルを用い、そのノードにより使用金額を決定することにより、一回発行された電子現金を発行時に決められた額になるまで、何回も分割して利用できる。

【図面の簡単な説明】

【図1】この発明が適用されるシステム例を示すブロック図。

【図2】利用許可証発行手続における交信例を示す図。

【図3】利用者側装置における利用許可証発行処理の構成を示すブロック図。

【図4】銀行側装置における利用許可証発行処理の構成を示すブロック図。

【図5】電子現金発行手続における交信例を示す図。

【図6】 A, B はそれぞれ電子現金発行処理における利用者側装置および銀行側装置の各構成を示すブロック

図。

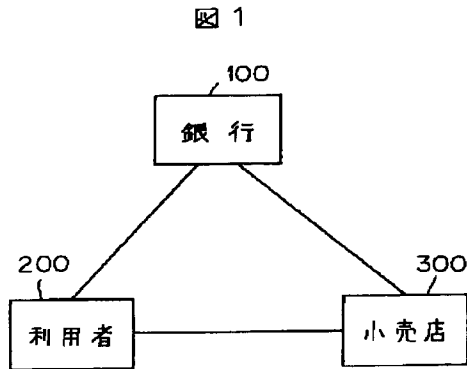
【図7】電子現金の階層的構造テーブルを示す図。

【図8】この発明による電子現金の利用手続における通信例を示す図。

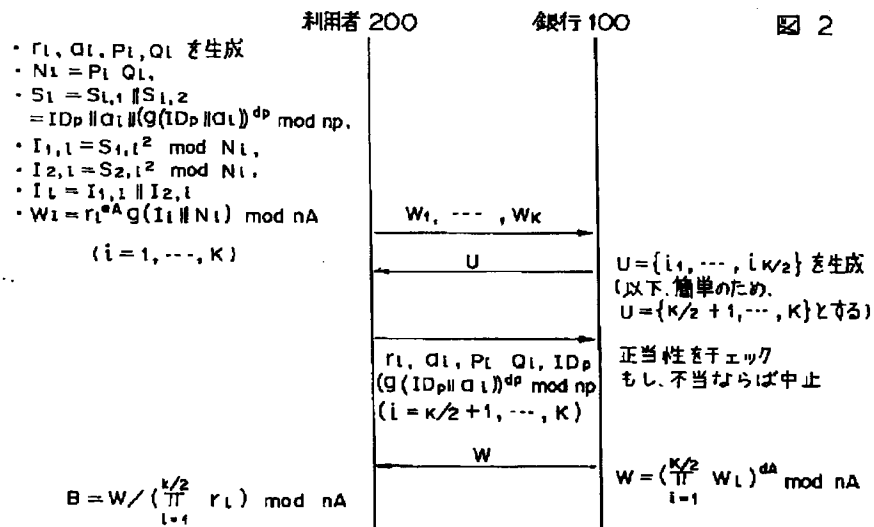
*【図9】図8の通信における利用者側装置での電子現金利用処理の構成を示すブロック図。

*【図10】図8の通信における小売店側装置での電子現金利用処理の構成を示すブロック図。

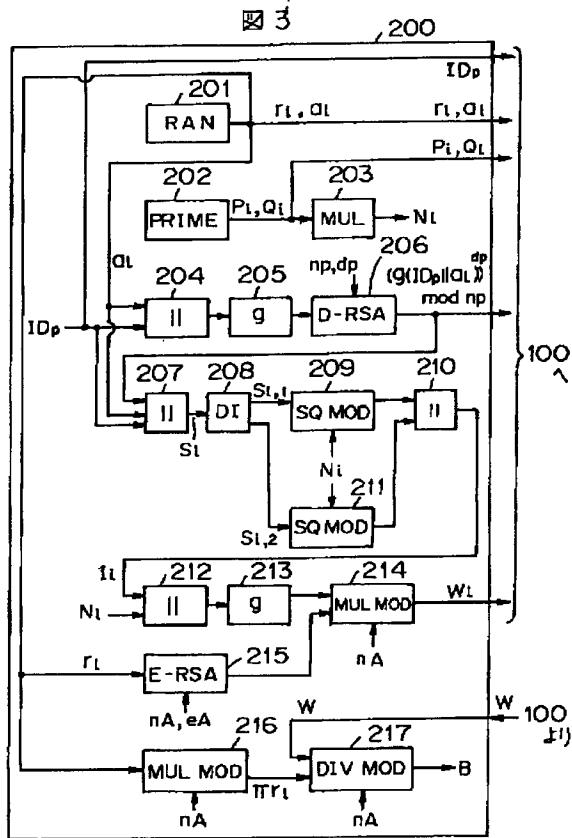
【図1】



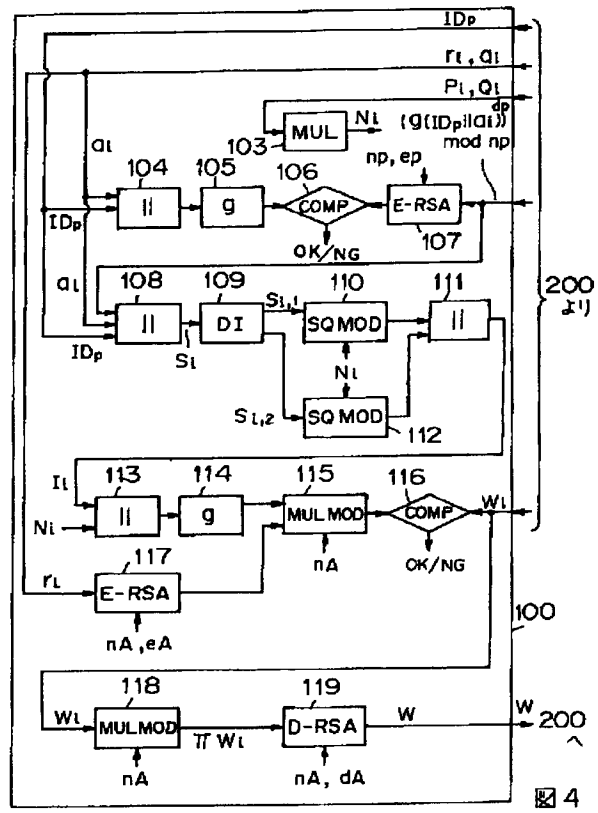
【図2】



【図3】

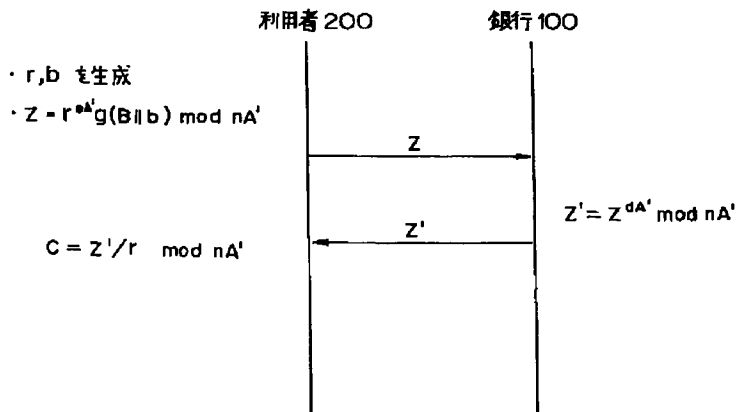


【図4】

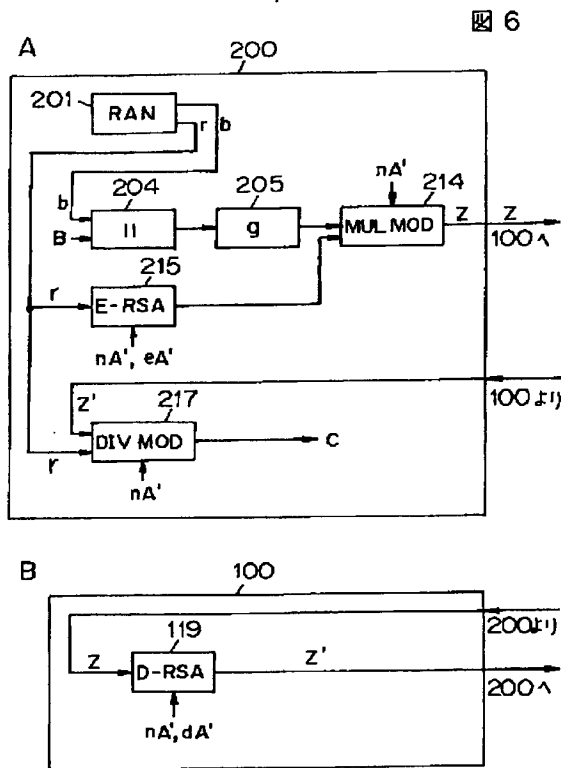


【図5】

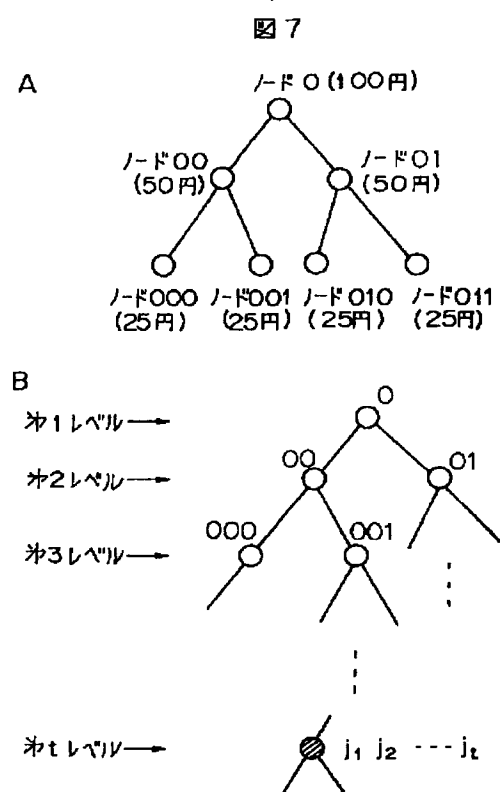
図5



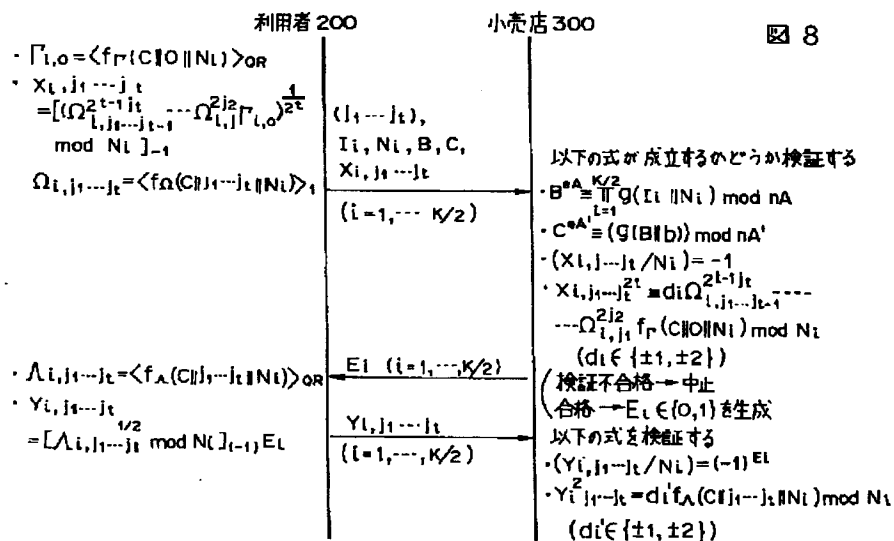
【図6】



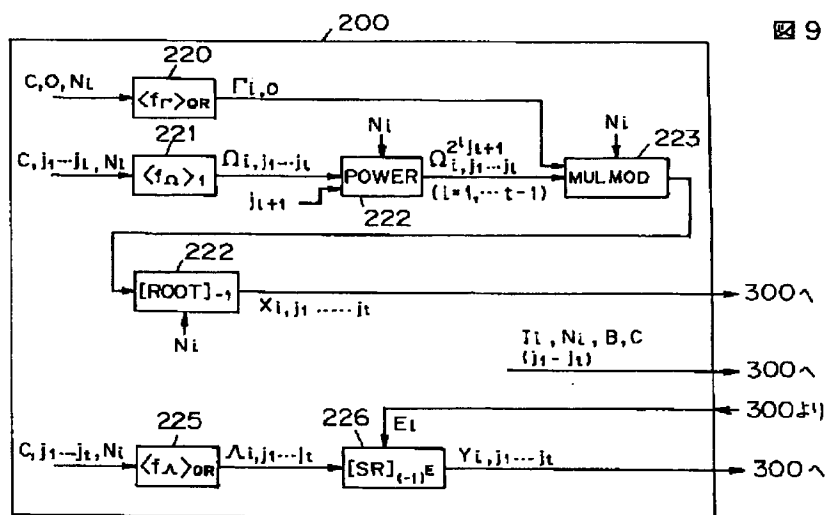
【図7】



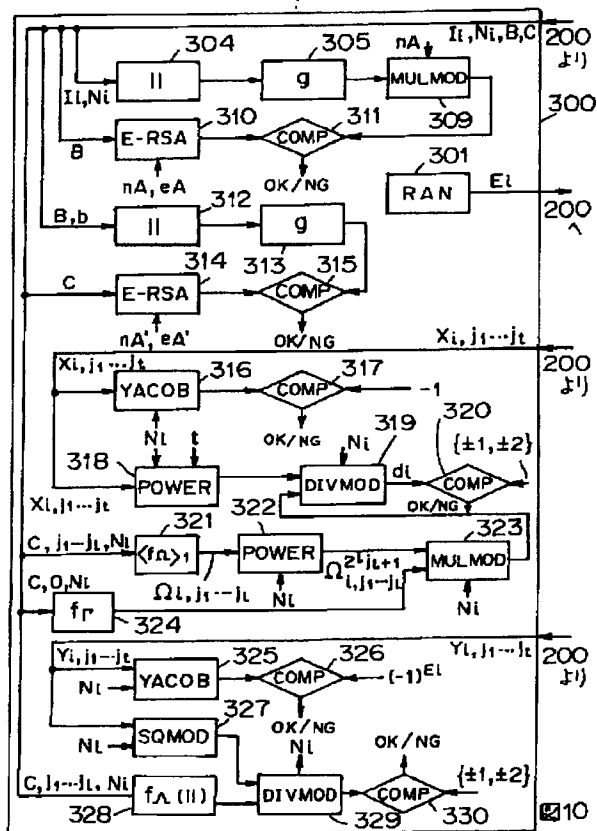
【図8】



【図9】



【図10】



フロントページの続き

(51)Int.Cl.⁶

識別記号

庁内整理番号

F I

G 0 7 F 7/08

技術表示箇所

B